AN - 1998-428718 [37]

XP - N1998-334669

TI - Digital signature generating method for message - using secret key containing several large primary numbers and forming signature using zero point of polynom using random permutation polynom

DC - W01

PA - (DEBP) DEUT TELEKOM AG

IN - HUBER K; SCHWENK J

NP - 4

NC - 24

PN - **DE19703929** A1 19980806 DW1998-37 H04L-009/30 4p *
AP: 1997DE-1003929 19970204

WO9834373 A1 19980806 DW1998-37 H04L-009/32 Ger
AP: 1998WO-EP00303 19980121
DSNW: CA CN JP KR TR US
DSRW: AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE

EP-958676 A1 19991124 DW1999-54 H04L-009/32 Ger
FD: Based on WO9834373
AP: 1998EP-0904107 19980121; 1998WO-EP00303 19980121
DSR: AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

JP2001509914 W 20010724 DW2001-47 G09C-001/00 20p
FD: Based on WO9834373
AP: 1998JP-0532501 19980121; 1998WO-EP00303 19980121

PR - 1997DE-1003929 19970204

IC - G09C-001/00 H04L-009/30 H04L-009/32

AB - DE19703929 A
The method involves using a secret key containing several large primary numbers (p,q). The zero point of a polynom P(x)-m modulo n forms the signature, with P (x) a random permutation polynom modulo n.
Preferably, the product n is formed from the primary numbers, and the signature is generated as s = b*u*p + a*V*q mod n, while starting from the equation 1 = u * p+v * q the values u are calculated by widened Euclidic algorithm. The values a, b are obtained from the equation ggT(P(x)-m, x exp p -x) mod p = x-a; ggT(P(x)-m, x exp q -x) mod q = x-b.
USE - E.g. for public key signature processes in data communication.
ADVANTAGE - Provides always valid signature. (Dwg.0/0)

MC - EPI: W01-A05B

UP - 1998-37

UE - 1998-37; 1999-54; 2001-47